## REMARKS

Claims 1-143 are pending in this application. By this Amendment, claims 1, 5, 6, 10, 11 and 15 are amended. Support for the amendments can be found in Applicants' disclosure at least on page 7, lines 15-17 of the specification. No new matter is added. A Request for Continued Examination is attached. Reconsideration of the application in view of the above amendments and the following remarks is respectfully requested.

The Office Action, on page 3, rejects claims 1, 4-6, 9-11 and 14-17 under 35 U.S.C. §102(b) over Cisco (http://community.roxen.com/developers/idocs/rfc/rfc2305.html). The Office Action, on page 6, rejects claims 1, 6, 11 and 16 under 35 U.S.C. §102(a) over Windows 95 (http://www.microsoft.com/technet/archive/win95/rk27_fax.mspx?mfr=true). The rejections are respectfully traversed.

Independent claim 1 recites, among other features, a control method of an Internet facsimile comprising receiving electronic mail containing a control command and an encrypted password relating to the control command for indicating a facsimile communication function, wherein the facsimile communication function is a command for indicating a confidential communication function, a bulletin board communication function, or a relay broadcast communication function. Independent claims 6 and 11 recite similar features. Cisco and Windows 95, either individually or in combination, fail to teach, or to have suggested, a control method of an Internet facsimile that includes the above-described features recited in independent claims 1, 6 and 11.

The Office Action, on page 6, alleges that Windows 95 teaches all of the features recited in claim 1. Windows 95 teaches fax software that sends and receives faxes in editable files from a computer. The Microsoft fax software has a feature to control or restrict access to the shared fax service. In particular, Windows 95 teaches a feature to control or restrict access to the shared fax service, by defining a shared fax password. Windows 95 teaches that

when a message is received, Microsoft fax uses a public key and a recipient's private key to decrypt it. Windows 95 teaches defining a password to share a facsimile server (see the paragraph bridging pages 7 and 8). Windows 95 also teaches encrypting a facsimile with a private key/public key (see page 9). For example, Windows 95 teaches that when an electronic mail containing a password is sent using S-MIME, a destination would receive the "electronic mail containing the encrypted password" and decrypt the "encrypted password." However, even if a received electronic mail contains an encrypted password, Windows 95 does not teach, nor can it reasonably be considered to have suggested, any use for the decrypted password.

In this regard, Windows 95 cannot reasonably be considered to teach, or to have suggested, receiving electronic mail containing an encrypted password relating to a control command for indicating a facsimile communication function; and transferring an electronic mail document by facsimile following the control command using the decrypted password. Windows 95 fails to disclose an encrypted password key that relates to the control command feature, as recited n independent claims 1, 6 and 11.

The Office Action, on page 4, asserts that Cisco, at section 5.3.2, teaches all of the features recited in claim 1. Cisco, in section 1 and section 5.2.1, teaches that electronic mail messages should be provided with a method of preventing the disclosure of sensitive information. However, at section 5.2.3, Cisco indicates that there are no standard mechanisms for protecting such information. Cisco indicates that the available non-standard techniques are out of band communications of authorization information. Cisco, at section 5.2.3 teaches that "use of encrypted data in special fields is the available non-standard techniques." In section 5.3.2, Cisco, merely teaches that message encryption, such as PGP-MIME and S-MIME is used to provide end-to-end encryption of the entire message text. Cisco merely teaches the use of PGP-MIME and S-MIME to identify a transmission source.

Section 5.3.2 of Cisco does not disclose or suggest transferring an electronic mail document by facsimile following the control command using the decrypted password. Cisco fails to teach, or to have suggested, an encrypted password key that relates to the control command feature, as recited n independent claims 1, 6 and 11.

Accordingly, Cisco and Windows 95, either individually or in combination, would not have suggested receiving an electronic mail message containing both a control command and an encrypted key that relates to the control command, wherein the control command is for indicating a facsimile communication function and is a command for indicating a confidential communication function, a bulletin board communication function, or a relay broadcast communication function. For at least the foregoing reasons, neither Cisco nor Windows 95 can reasonably be considered to teach, or to have suggested, the combinations of all of the features positively recited in independent claims 1, 6 and 11.

Independent claim 16 recites a communication control section for transferring the received electronic mail by facsimile over the telephone network only if the determination section determines that the transmission source is identified correctly. Neither Cisco nor Windows 95 can reasonably be considered to have suggested all of these features.

With respect to Cisco, the Office Action asserts that sections 5.2.1, 5.2.3 and 5.2.4 teaches the above-recited features recited in claim 16. This assertion is unreasonable for the following reasons.

Sections 5.2.1, 5.2.3 and 5.2.4 of Cisco do not relate to the transferring of the received electronic mail. Cisco, at section 1 and section 5.2.1, merely teaches that electronic mail messages should be provided with a method of preventing the disclosure of sensitive information. Cisco, at section 5.2.3, merely teaches that there are no standard mechanisms for protecting such information, and that the "use of encrypted data in special fields is the available nonstandard technique." Further, Cisco, at section 5.2.4, merely teaches that there is

a legal requirement that the sender be disclosed on a facsimile message. Based on the disclosure of these sections, Cisco cannot reasonably be considered to teach, or to have suggested, a communication control section for transferring the received electronic mail by facsimile over the telephone network only if the determination section determines that the transmission source is identified correctly.

With respect to Windows 95, the Office Action broadly asserts that http://www.microsoft.com/technet/archive/win95/rk27_fax.mspx?mfr=true teaches all of the features recited in claim 16 including a communication control section for transferring the received electronic mail by facsimile over the telephone network only if the determination section determines that the transmission source is identified correctly. This assertion relies on an improper construction of the disclosure of http://www.microsoft.com/technet/archive/win95/rk27_fax.mspx?mfr=true. This site of Windows 95 only teaches the option of sending a digitally signed fax so that a recipient can verify that the purported sender of the fax is the actual sender (see, e.g., page 9). There is no teaching or suggestion of transferring the received electronic mail by facsimile over the telephone network only if the determination section determines that the transmission source is identified correctly. For at least these reasons, the rejection of claim 16 over Windows 95 is unreasonable.

Further, claims 4, 5, 9, 10, 14, 15 and 17 are also not taught by Cisco for at least the respective dependence of each of these claims on allowable base claims, as well as for the separately patentable subject matter that each of these claims recites.

Accordingly, reconsideration and withdrawal of the rejection of claims 1, 4-6, 9-11 and 14-17 under 35 U.S.C. §102(b) as being anticipated by Cisco, and the rejection of claims 1, 6, 11 and 16 under 35 U.S.C. §102(a) as being anticipated by Windows 95 are respectfully requested.

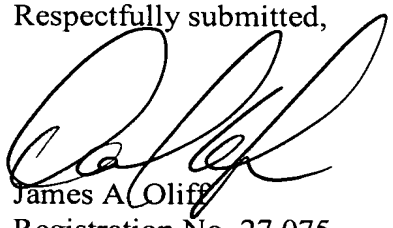
The Office Action, on page 7, rejects claims 2, 3, 7, 8, 12 and 13 under 35 U.S.C. §103(a) over Cisco (http://community.roxen.com/developers/idocs/rfc/rfc2305.html). The rejection is respectfully traversed.

Claims 2, 3, 7, 8, 12 and 13 also would not have been suggested by Cisco for at least the respective dependence of these claims directly on an allowable base claim, as well as for the separately patentable subject matter that each of these claims recites.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-17 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Daniel A. Tanner, III
Registration No. 54,734

JAO:DAT/clf

Date: March 21, 2008

Attachment:
Request for Continued Examination

**OLIFF & BERRIDGE, PLC**
**P.O. Box 19928**
**Alexandria, Virginia 22320**
**Telephone: (703) 836-6400**

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461